WE CLAIM:

1. A method of managing a communication with a mobile device over a network, comprising:

receiving a request from the mobile device, wherein the request includes associated information;

determining at least one level of trust based, in part, on the associated information; and

determining at least one device signature for the mobile device based on the at least one level of trust.

2. The method of Claim 1, further comprising:

receiving gateway information, wherein the gateway information is associated with a carrier gateway for the mobile device; and

determining the at least one level of trust based, in part, on the associated information and the gateway information.

3. The method of Claim 1, wherein the associated information comprises at least one of a device identifier, user agent information, and an indication that the mobile device is enabled to accept a cookie.

4. The method of Claim 3, wherein the associated information further comprises at least one of a gateway group identifier, and a subscription identifier.

5. The method of Claim 1, wherein the associated information further comprises an end-user identifier.

6. The method of Claim 1, wherein the associated information further comprises a subscription identifier associated with the mobile device that is based on at least one of a Mobile Identification Number, an Electronic Serial Number, and an application serial number.

7. The method of Claim 1, wherein determining the at least one level of trust further comprises:

if the associated information comprises a device identifier and trustworthy gateway information, determining a first level of trust.

8. The method of Claim 1, wherein determining the at least one level of trust further comprises:

if the associated information indicates the mobile device is enabled to accept a cookie, determining a second level of trust.

9. The method of Claim 1, wherein determining the at least one level of trust further comprises:

if the associated information indicates the mobile device is enabled to use a URL, determining a third level of trust.

10. The method of Claim 1, wherein determining at least one device signature further comprises:

if a first level of trust is determined, determining a first tier device signature based, in part, on a hash of at least one of a subscription identifier, a gateway group identifier, a user agent identifier, and a time stamp.

11. The method of Claim 1, wherein determining at least one device signature further comprises:

if a second level of trust is determined, determining a second tier device signature based, in part, on a hash of at least one of a cookie, a gateway group identifier, a user agent identifier, and a time stamp.

12. The method of Claim 1, wherein determining at least one device signature further comprises:

if a third level of trust is determined, determining a third tier device signature based, in part, on a hash of at least one of a gateway group identifier, a user

agent identifier, a server identifier, a process identifier, a random number, and a time stamp.

13. The method of Claim 12, wherein determining the third tier device signature further comprises including the third tier device signature in a munged URL.

14. The method of Claim 1, wherein determining at least one device signature further comprises employing a hash function selected from at least one of a Message Digest, a Secure Hash Algorithm (SHA), Digital Encryption Standard (DES), triple-DES, Hash of Variable Length (HAVAL), RIPEMD, and Tiger hash function.

15. The method of Claim 1, further comprising expiring the at least one device signature based, in part, on a predetermined period of time associated with each of the at least one device signature.

16. The method of Claim 1, further comprising:

if the at least one device signature has expired, determining if the expired device signature is to be rolled over, and

if the expired device signature is to be rolled over, extending a validity period associated with the expired device signature.

17. The method of claim 16, wherein determining if the expired device signature is to be rolled over further comprises evaluating at least one of a condition, event, change in an identifier indicating a grouping of the gateway, and a time.

18. A client adapted for a mobile device to communicate with a server over a network, the client being configured to perform actions, comprising:

sending a request to the server for content, wherein the request includes an identifier associated with a user agent;

receiving at least one device signature associated with the mobile device, wherein the at least one device signature is based on at least one level of trust.

19. The client of Claim 18, wherein the client is configured to perform actions, further comprising:

providing a device identifier based on at least one of a Mobile Identification Number, an Electronic Serial Number, and an application serial number.

20. The client of Claim 18, wherein receiving the at least one device signature further comprises:

if the at least one device signature is based on a first level of trust, receiving a first tier device signature based, in part, on a hash of at least one of a subscription identifier, a gateway group identifier, the user agent identifier, and a time stamp.

21. The client of Claim 18, wherein receiving the at least one device signature further comprises:

if the at least one device signature is based on a second level of trust, receiving a second tier device signature based, in part, on a hash of at least one of a cookie, a gateway group identifier, the user agent identifier, and a time stamp.

22. The client of Claim 18, wherein receiving the at least one device signature further comprises:

if the at least one device signature is based on a third level of trust, receiving a third tier device signature based, in part, on a hash of at least one of a gateway group identifier, a user agent identifier, a server identifier, a process identifier, a random number, and a time stamp.

23. The client of Claim 18, wherein sending the request further comprises sending the request to a carrier gateway, wherein the carrier gateway is configured to perform actions, comprising:

modifying the request to include at least one of a subscription identifier associated with the mobile device, and a gateway identifier;

forwarding the modified request to the server;

receiving the at least one device signature from the server; and

forwarding the at least one device signature to the mobile device.

24. The client of Claim 18, wherein receiving the at least one device signature further comprises, if the request indicates the mobile device is enabled to accept a cookie, associating the cookie with the at least one device signature.

25. The client of Claim 18, wherein receiving the at least one device signature further comprises, associating a munged Uniform Resource Locator (URL) with the at least one device signature.

26. A server for managing a communication with a mobile device over a network, comprising:

a transceiver for receiving a request from the mobile device and for sending at least one device signature to the mobile device; and

a transcoder that is configured to perform actions, including:

receiving the request from the mobile device, wherein the request includes associated information;

determining at least one level of trust based, in part, on the associated information; and

determining the at least one device signature for the mobile device based on the at least one level of trust.

27. The server of Claim 26, wherein the transcoder is configured to perform further action, comprising:

receiving gateway information, wherein the gateway information is associated with a carrier gateway for the mobile device; and

determining the at least one level of trust based, in part, on the associated information and the gateway information.

28. The server of Claim 26, wherein determining the at least one device signature further comprises:

if a first level of trust is determined, determining a first tier device signature based, in part, on a hash of at least one of a subscription identifier, a gateway group identifier, a user agent identifier, and a time stamp.

29. The server of Claim 26, wherein determining the at least one device signature further comprises:

if a second level of trust is determined, determining a second tier device signature based, in part, on a hash of at least one of a cookie, a gateway group identifier, a user agent identifier, and a time stamp.

30. The server of Claim 26, wherein determining the at least one device signature further comprises:

if a third level of trust is determined, determining a third tier device signature based, in part, on a hash of at least one of a gateway group identifier, a user agent identifier, a server identifier, a process identifier, a random number, and a time stamp.

31. The server of Claim 26, wherein determining the at least one level of trust further comprises determining a first level of trust based at least one of a gateway group identifier, a subscription identifier, a user agent, and a security level associated with the request from the mobile device.

32. The server of Claim 26, wherein determining the at least one level of trust further comprises determining a second level of trust based at least one of a gateway identifier, a user agent, and whether the mobile device is enabled to accept a cookie,.

33. The server of claim 26, wherein determining the at least one level of trust further comprises determining a third level of trust if the mobile device is enabled to interact with a URL.

34. The server of claim 26, wherein the transcoder is configured to perform further actions, comprising:

determining if at least one device signature has expired device, and

if the expired device signature is to be rolled over, extending a validity period associated with the expired device signature.

35. A system for managing a communication with a mobile device over a network comprising:

the mobile device configured to provide information associated with the mobile device; and

a server, coupled to the carrier gateway, that is configured to receive the associated information and to perform actions, including:

determining at least one level of trust based, in part, on the associated information; and

determining at least one device signature for the mobile device based on the at least one level of trust.

36. The system of Claim 35, wherein determining the at least one device signature further comprises determining a tier 1 device signature based, in part, on a hash of at least one of a subscription identifier, a gateway group identifier, a user agent identifier, and a time stamp.

37. The system of Claim 35, wherein determining the at least one device signature further comprises determining a tier 2 device signature based, in part, on a hash of at least one of a cookie, a gateway group identifier, a user agent identifier, and a time stamp.

38. The system of Claim 35, wherein determining the at least one device signature further comprises determining a tier 3 device signature based, in part, on a hash of at least one of a gateway group identifier, a user agent identifier, a server identifier, a process identifier, a random number, and a time stamp.

39. The system of Claim 38, wherein the tier 3 device signature is provided to the mobile device through a munged URL.

40. The system of Claim 35, further comprising:

a carrier gateway, coupled to the mobile device, that is configured to receive the associated information, and provide the associated information and gateway information related to the carrier gateway.

41. A modulated data signal for communicating with a mobile device, the modulated data signal comprising the actions of:

receiving a request from the mobile device, wherein the request includes associated information;

sending at least one device signature to the mobile device based on the at least one level of trust that is determined, in part, using the associated information.

42. The modulated data signal of Claim 41, wherein determining the at least one device signature further comprises:

if a first level of trust is determined, determining a first tier device signature based, in part, on a hash of at least one of a subscription identifier, a gateway group identifier, a user agent identifier, and a time stamp.

43. The modulated data signal of Claim 41, wherein determining the at least one device signature further comprises:

if a second level of trust is determined, determining a second tier device signature based, in part, on a hash of at least one of a cookie, a gateway group identifier, a user agent identifier, and a time stamp.

44. The modulated data signal of Claim 41, wherein determining the at least one device signature further comprises:

if a third level of trust is determined, determining a third tier device signature based, in part, on a hash of at least one of a gateway group identifier, a user agent identifier, a server identifier, a process identifier, a random number, and a time

45. An apparatus for communicating with a mobile device, comprising:

a means for receiving a request from a mobile device, wherein the request includes associated information;

a means for determining at least one level of trust based, in part, on the associated information; and

a means for determining at least one device signature for the mobile device based, in part, on the at least one level of trust.